## REMARKS

The Applicants and undersigned thank Examiner Pich for a careful review of this application. Upon entry of this amendment, Claims 1, 4, 6, 49, and 60-80 are pending in the application, with Claims 1, 49, 66, and 71 being the independent clams. Applicants have amended Claims 1, 6, 49, 63, 64, 66, 68, 70-73, and 75 herein. Applicants have added new claims 76-80 herein to provide an additional scope of protection commensurate with the original disclosure. The new claims and amendments to the claims are fully supported by the specification and do not include new matter. Reconsideration of the present application is respectfully requested in light of the above amendments to the claims and the foregoing remarks.

### I. Summary of the Office Action

In the Office Action, the Examiner asserts that the declaration is defective and that a new oath or declaration is required. Claims 49 and 62-70 were rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. Claims 1, 4, 6, 49, and 60-75 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent No. 6,088,804 to Hill ("*Hill*").in view of U.S. Patent No. 5,375,199 to Harrow ("*Harrow*").

### II. Remarks Regarding Declaration

In the Office Action, the Examiner asserts that the declaration is defective and that a new oath or declaration is required. In particular, the Examiner asserts that the declaration is defective because the declaration submitted on September 24, 2001 identifies all the inventors as the sole or first inventor. The Examiner further asserts that it is unclear who should be listed as the first inventor and it is further unclear if all people signing their respective copies of the declaration understand that they are not the sole inventor of the invention being claimed.

Applicants submit that the declaration submitted on September 24, 2001 ("declaration) is not defective. The second sentence of the first paragraph of the declaration clearly states, "I believe I am an original, first, and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled: System and Method for Managing Security Events on a Network, the specification of which was filed with the United States Patent and Trademark Office on April 27, 2001, and assigned Serial Number 09/844,448." (emphasis added). This sentence clearly identifies each inventor as a joint inventor of the subject matter which is claimed, rather than a sole inventor.

It is also clear that Gregory Neil Houston should be listed as the first inventor as Gregory Neil Houston is listed first in the declaration. See MPEP 605.04(f):

> The order of names of joint patentees in the heading of the patent is taken from the order in which the type-written names appear in the original oath or declaration.

Further, the declaration was considered and accepted by the United States Patent Office in connection with its assessment of a Petition For Filing By Other Than All The Inventors Under 37 C.F.R. 1.47(a) that was granted on August 15, 2002.

In view of the foregoing, Applications respectfully submit that the declaration is not defective.

## III. Remarks Regarding Claim Rejections Under 35 U.S.C. § 101

In the Office Action, the Examiner rejected Claims 49 and 62-70 under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. In particular, the Examiner asserts that Claims 49 and 66 are directed to a computer program product comprising a computer-readable storage medium and that the specification as originally filed fails to set forth the metes and bounds of what is meant to be encompassed by the term "computer-readable storage medium." The Examiner further asserts that it would have been reasonable to interpret the term as encompassing signals per se having stored thereon or encoded with computer readable program code. Applicants respectfully traverse these rejections.

### A. Claims 49 and 62-65

Applicants submit that Claims 49 and 62-65 are not directed to a computer program product. Instead, Claims 49 and 62-65 are directed to a method for managing security event data collected from a plurality of security devices in a distributed computing environment. Therefore, Applicants submit that this rejection of Claims 49 and 62-65 is improper and respectfully requests that the Examiner withdraw this rejection of Claims 49 and 62-65.

### B. Claims 66-70

Applicants present with this Response an amendment to the Detailed Description in the form of the new paragraphs set forth above and an amendment to the drawings in the form of a new Figure 22 submitted herewith. Applicants submit that neither of these amendments presents new matter.

New Figure 22 sets forth conventional components of a computing system known to those of ordinary skill in the art. It is well known to those of ordinary skill in the art that conventional computing systems include computer-readable storage devices for storing programs and CPUs and computer-readable memories for processing the stored programs. These components also were generally described throughout the originally-filed specification. The new paragraphs set forth above describe the general operation of the components illustrated in Figure 22. The operation of the components as described in the new paragraphs is known to those of ordinary skill in the art. Furthermore, support for the operation of the components can found throughout the originally-filed specification, including page 5, line 20 - page 6, line 20. For example, the Applicants' original specification recites, "In a distributed computing environment, program modules may be physically located in different local and remote memory storage devices. Execution of the program modules may occur locally in a stand-alone manner or remotely in a client/server manner." See Applicants' original specification, page 5, lines 23-26. In another example, the Applicants' original specification recites, "The detailed description which follows is represented largely in terms of processes and symbolic representations of operations in a distributed computing environment by conventional computer components, including database servers, application servers, mail servers, routers, security devices, firewalls, clients, workstations, memory storage devices, display devices and input devices. The processes and operations performed by the computer include the manipulation of signals by a client or server and the maintenance of these signals within data structures resident in one or more of the local or remote memory storage devices. Such data structures impose a physical organization upon the collection of data stored within a memory storage device and represent specific electrical and magnetic elements. See Applicants' original specification at page 5, line 28 - page 6, line 9.

Support is also found from the well known and inherent manner of storing and executing a program in a computer:

"MPEP 2163.07(a) Inherent Function, Theory, or Advantage

> By disclosing in a patent application a device that inherently performs a function or has a property, operates according to a theory or has an advantage, a patent application necessarily discloses that function, theory or advantage, even though it says nothing explicit concerning it. The application may later be amended to recite the function, theory or advantage without introducing prohibited new matter. *In re Reynolds*, 443 F.2d 384, 170 USPQ 94 (CCPA 1971); *In re Smythe*, 480 F. 2d 1376, 178 USPQ 279 (CCPA 1973). "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (citations omitted)."

The computer product claims 66-75 comply with 35 U.S.C. § 101 because these claims recite a "computer-readable tangible storage device" that comprises various computer readable program code stored on the computer-readable tangible storage device. A "tangible storage device" precludes a carrier wave because a carrier wave is not a tangible device and does not store data. Also, a communication cable (wire or fiber optic) is not a storage device; rather the communication cable propagates signals. Also, a propagating signal is not stored on a device, rather it propagates along the device.

In view of the foregoing, Applicants submit that the original specification fully supports a computer program product comprising program instructions stored on a computer-readable storage device, as set forth in Claims 66-75. Accordingly, Applicants request reconsideration and withdrawal of this rejection of Claims 66-70.

## IV. <u>Remarks Regarding Claim Rejections Under 35 U.S.C. § 103</u>

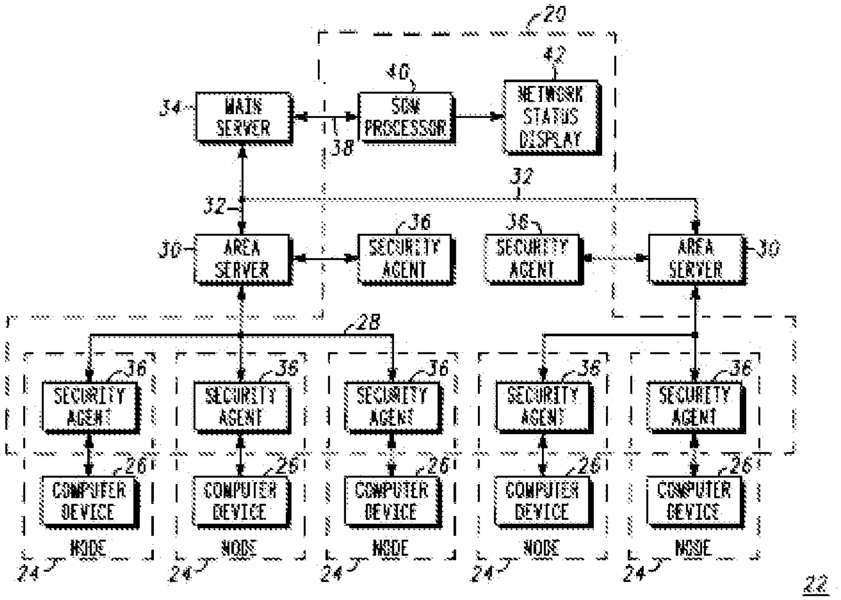
In the Office Action, the Examiner rejected Claims 1, 4, 6, 49, and 60-75 under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Hill* in view of *Harrow*. Applicants respectfully traverse these rejections.

### A. <u>Independent Claim 1</u>

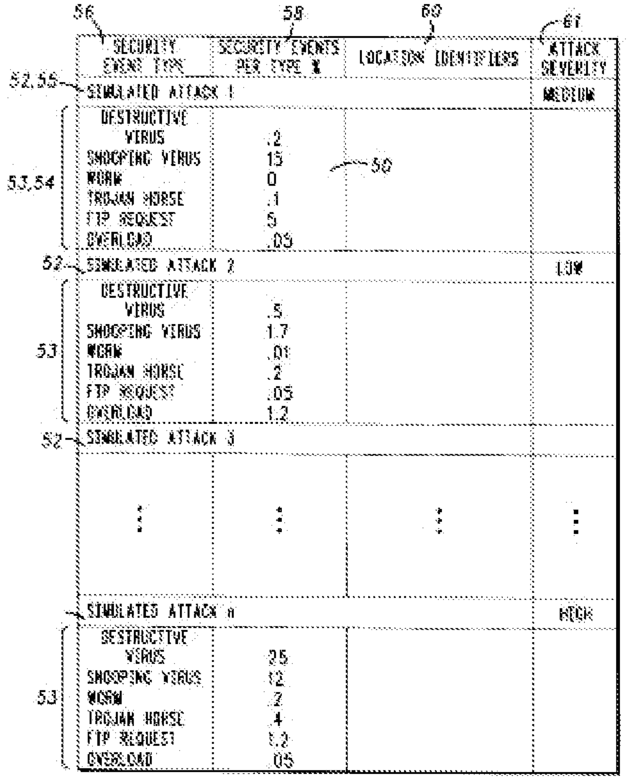
Applicants submit that the combination of *Hill* and *Harrow* fails to teach, suggest, or make obvious all of the elements of independent Claim 1, as amended. In particular, the combination fails to teach, suggest, or make obvious the features of (1) the computer presenting a user interface via the display for configuring an event data report that identifies a portion of the security event data; (2) the computer receiving a selection via the user interface of one or more user-configurable variables operable for filtering the security event data, the user-configurable variables comprising at least one of a location of a security event, a source of a security event, and a destination address of a security event; and (3) the computer filtering the collected security event data using the one or more user-configurable variables to produce result data for the event data report, the filtering comprising passing collected security event data that matches the user-configurable variables as result data while blocking collected security event data that does not match the user-configurable variables from the result data, as recited in amended Claim 1.

In the Office Action, the Examiner asserts that *Hill* teaches filtering collected security event data using one or more user-configurable variables to produce the result data for an event data report, as recited in Claim 1. The Examiner further asserts that although *Hill* does not explicitly disclose the computer presenting a user interface via the display for configuring the event data report and the computer receiving the selection via the user interface, the particular attacks mapped and responded to by *Hill's* invention is configurable (i.e., by a user) and that some method which allows the user to make selections must be utilized by *Hill's* invention. The Examiner further asserts that *Harrow* discloses a system in which a computer presents a user interface via a display for configuring which activities to monitor and the computer receiving the selection via the user interface.

As Applicants understand, the *Hill* reference describes a dynamic network security system (20) that responds to a security attack on a computer network (22) having a multiplicity of computer nodes (24). The security system (20) includes a plurality of security agents (36) that concurrently detect occurrences of security events on associated computer nodes (24). A processor (40) processes the security events that are received from the security agents (36) to form an attack signature of the attack. A network status display (42) displays multi-dimensional attack status information representing the attack in a two dimensional image to indicate the overall nature and severity of the attack. See Figure 1 of the *Hill* system reproduced below.



As shown in Figure 3 of the *Hill* reference below, a database (48) maintains the simulated attack information for a plurality of simulated attacks (52). Each of the simulated attacks (52) is a prediction of an attack type that may occur on network (22). Simulated attacks (52) are generated by an operator and stored in database (48). Each simulated attack (52) contains a training signature (53) that is defined by a plurality of security events (50) of at least one security event type (56). The training signatures are generated by an operator and include at least one security event type (56), a representation (58) of the number of nodes (24) affected by each security event type, a location identifier (60) that identifies the nodes (24) where security events may take place, and an attack severity (61) for each simulated attack.



| SECURITY EVENT TYPE | SECURITY EVENTS PER TYPE % | LOCATION IDENTIFIERS | ATTACK SEVERITY |
|---|---|---|---|
| SIMULATED ATTACK 1 | | | MEDIUM |
| DESTRUCTIVE VIRUS | .2 | | |
| SNOOPING VIRUS | 15 | | |
| WORM | 0 | | |
| TROJAN HORSE | .1 | | |
| FTP REQUEST | 5 | | |
| OVERLOAD | .05 | | |
| SIMULATED ATTACK 2 | | | LOW |
| DESTRUCTIVE VIRUS | .5 | | |
| SNOOPING VIRUS | 1.7 | | |
| WORM | .01 | | |
| TROJAN HORSE | .2 | | |
| FTP REQUEST | .05 | | |
| OVERLOAD | 1.2 | | |
| SIMULATED ATTACK 3 | | | |
| ⋮ | ⋮ | ⋮ | ⋮ |
| SIMULATED ATTACK n | | | HIGH |
| DESTRUCTIVE VIRUS | 25 | | |
| SNOOPING VIRUS | 12 | | |
| WORM | .2 | | |
| TROJAN HORSE | .4 | | |
| FTP REQUEST | 1.2 | | |
| OVERLOAD | .05 | | |

*FIG. 3*

An SOM processor (40) performs each of the simulated attacks and maps the training signatures into a network status display (42). Figure 4, reproduced below, shows a display map (66) which forms a portion of network display (42). A self organizing map algorithm plots a vector representative of the training signatures onto the two dimensional array of display cells (68) in such a way that vectors projected onto adjacent display cells (68) are more similar than vectors projected onto distant display cells (68). Display map (66) includes a center region (70), a middle region (72), and an outer region (74). Display cells (68) within center region (70) represent a computer network under an attack of low severity, display cells (68) in middle region represent a computer under an attack of medium severity, and display cells (68) in outer region (74) represent a computer under an attack of high severity. Regions (70), (72), and (74) are further subdivided into subregions (76) that are configured to indicate attack type.

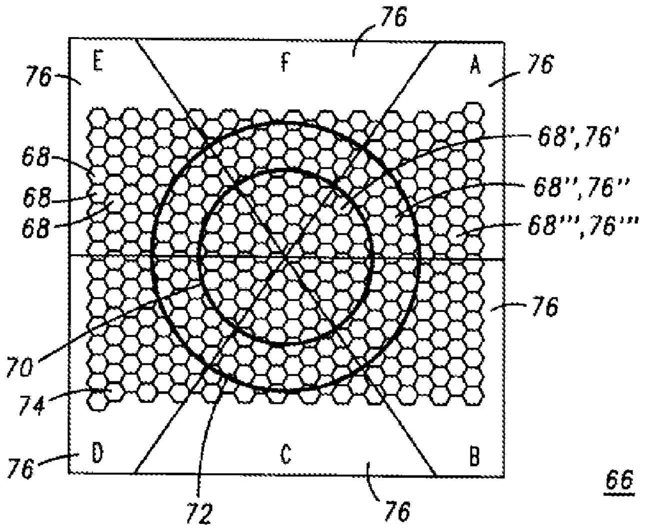
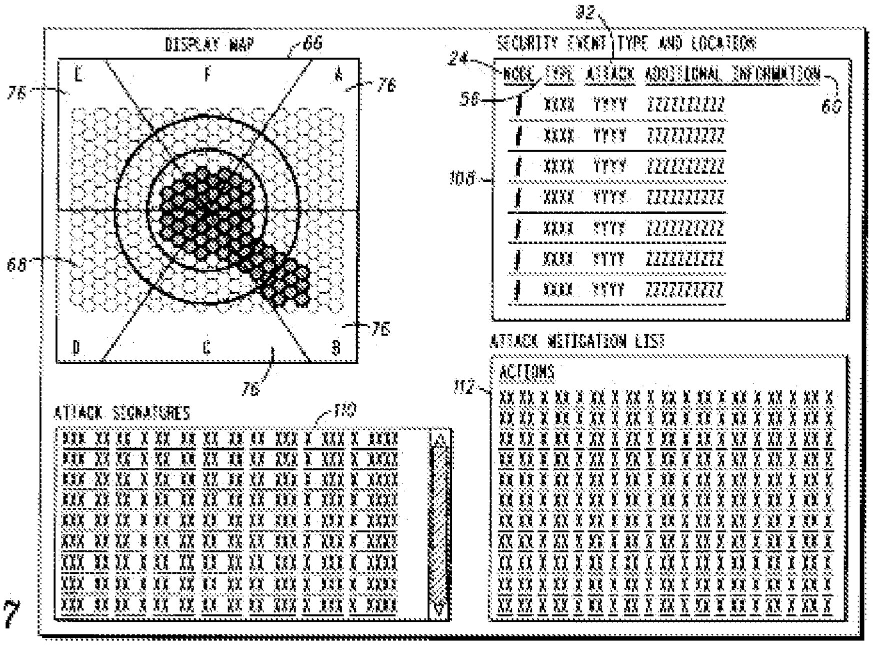


FIG. 4

Following system training process (44), dynamic network security system (20) is configured to respond to a plurality of attacks on computer network (22). Information from security agents (36) about security events are combined at area servers (30) and combined to form an attack signature. This attack signature constitutes a number of security events (50) shown in column (92) as percentage values, occurring at nodes (24) and categorized by security event types (56). The SOM processor (40) compares a vector representative of the attack signature to each training signature (53) as mapped in display map (66). A tack (102) selects one of the training signatures (53) that most closely resembles the attack signature. Following task (102), a task (104) displays attack status information and the mitigation list on network status display 42.

As shown in Figure 7 of the *Hill* reference below, a network status display (42) displays multi-dimensional attack status information in a two dimensional image to indicate the overall nature and severity of an attack. The network status display (42) presents a display map (66) and an attack status information list (108) showing security event type (56) and location identifiers (60) for an example attack (92). The network status display (42) also presents an attack signature log (110) which provides current and historical perspective on a given attack record at various sample times. The attack signatures in log (110) are the text equivalent of the two dimensional image as highlighted in display map (66). In addition, the network status display (42) includes an attack mitigation list (112) which is a catalogue of actions that a network manager may take in order to mitigate the example attack (92).



42

*FIG. 7*

In summary, the *Hill* reference teaches generating simulated attacks that may occur on the network. These simulated attacks comprise training signatures that define what types of security events are present in each attack. The training signatures are generated by an operator and include at least one security event type (56), a representation (58) of the number of nodes (24) affected by each security event type, a location identifier (60) that identifies the nodes (24) where security events may take place, and an attack severity (61) for each simulated attack. An SOM processor (40) uses the training signatures and vector representations of an attack signature to display the attack on a two dimensional map (66).

The *Hill* reference fails to teach, suggest, or make obvious, alone or in combination with *Harrow*, a computer filtering collected security event data using one or more user-configurable variables to produce the result data for an event data report, the filtering comprising passing collected security event data that matches the user-configurable variables as result data <u>while blocking collected security event data that does not match the user-configurable variables from the result data</u>. Instead, as described above, *Hill* displays attack signatures on a two dimensional display map based on the type of security event, the severity of the security event, and the similarity of that security event with other security events, using training signatures. *Hill* does not include any disclosure directed to filtering security event data to display security event data that matches user-configurable variables, while blocking the display of security event data that does not match the user-configurable variables. Instead, *Hill* is directed to tracking multiple security events that form an attack signature using a two dimensional map, without the capability of filtering out events based on user-configurable variables.

The Examiner asserts that the particular attacks mapped and responded to by *Hill's* invention are configurable and that some method which allows the user to make selections to thereby configure the event data report must be utilized by *Hill's* invention. Although *Hill* discloses that operators may generate simulated attacks having an attack signature that are used to train an SOM processor, these simulated attacks do not include user-configurable variables operable for filtering security event data to pass security event data that matches the user-configurable variables and block security event data that does not match the user-configurable variables. Instead, these security events are used to identify a location on a two dimensional display map for displaying an attack. *Hill* does not enable a user to select, using user-configurable variables, which portion of security event data is displayed in an event data report.

The Examiner further asserts that *Harrow* discloses a system in which a computer presents a user interface via a display for configuring which activities to monitor and the computer receiving the selection via the user interface. However, *Harrow* does not disclose a user interface for configuring an event data report for filtering security event data and for receiving a selection of one or more user-configurable variables for filtering the security event data, the user-configurable variables comprising at least one of a location of a security event, a source of a security event, and a destination address of a security event, as set forth in amended Claim 1. Instead, the system of *Harrow* provides two interactive icons that can be manipulated by a user to alter the view of information represented by the icons. See *Harrow*, Col. 3, lines 29-35. The first icon allows a user to select and display in an intuitive manner on a display device, information contained in a historical record, or log, of information, as well as real time information. See *Harrow*, Col. 3, lines 35-39. The second icon allows a user to set a range of values in relation to other currently displayed information and to view such relationships in an intuitive manner. See *Harrow*, Col. 3, lines 39-44.

Thus, Applicants submit that the combination of *Hill* and *Harrow* fails to teach, suggest, or make obvious the features of (1) the computer presenting a user interface via the display for configuring an event data report that identifies a portion of the security event data; (2) the computer receiving a selection via the user interface of one or more user-configurable variables operable for filtering the security event data, the user-configurable variables comprising at least one of a location of a security event, a source of a security event, and a destination address of a security event; and (3) the computer filtering the collected security event data using the one or more user-configurable variables to produce result data for the event data report, the filtering comprising passing collected security event data that matches the user-configurable variables as result data while blocking collected security event data that does not match the user-configurable variables from the result data, as recited in amended Claim 1. Accordingly, Applicants request reconsideration and withdrawal of this rejection of Claim 1.

### B. Independent Claim 49

The rejection of Claim 49 is traversed. Applicants submit that the combination of *Hill* and *Harrow* fails to teach, suggest, or make obvious all of the elements of independent Claim 49, as amended. In particular, the combination fails to teach, suggest, or make obvious the features of (1) the computer presenting a user interface via the display for configuring an event data report that identifies a portion of the security event data; (2) the computer receiving a selection via the user interface of one or more user-configurable variables operable for filtering the security event data, the user-configurable variables comprising at least one of a security event type, a priority of a security event, and an identification of a system that detected a security event; and (3) the computer filtering the stored security event data using the one or more user-configurable variables to produce result data for the event data report, the filtering comprising passing stored security event data that matches the user-configurable variables as result data while blocking stored security event data that does not match the user-configurable variables from the result data.

As described above with reference to the discussion of independent Claim 1, the combination of *Hill* and *Harrow* fails to teach, suggest, or make obvious a computer presenting a user interface for configuring an event data report that identifies a portion of security event data; or a computer receiving a selection via the user interface of one or more user-configurable variables operable for filtering the security event data. Furthermore, as described above with reference to the discussion of independent Claim 1, the combination of *Hill* and *Harrow* fails to teach, suggest or make obvious the computer filtering the collected security event data using the one or more user-configurable variables to produce result data for the event data report, the filtering comprising passing stored security event data that matches the user-configurable variables as result data while blocking stored security event data that does not match the user-configurable variables from the result data. Therefore, the combination of *Hill* and *Harrow* fails to teach, suggest, or make obvious the features of: (1) the computer presenting a user interface via the display for configuring an event data report that identifies a portion of the security event data; (2) the computer receiving a selection via the user interface of one or more user-configurable variables operable for filtering the security event data, the user-configurable variables comprising at least one of a security event type, a priority of a security event, and an identification of a system that detected a security event; and (3) the computer filtering the stored security event data using the one or more user-configurable variables to produce result data for the event data report, the filtering comprising passing stored security event data that matches the user-configurable variables as result data while blocking stored security event data that does not match the user-configurable variables from the result data.

Accordingly, Applicants submit that Claim 49 is patentable over the combination of references cited by the Examiner, and respectfully request the Examiner withdraw this rejection to Claim 49.

## C. <u>Independent Claims 66 and 71</u>

Independent Claims 66 and 71 recite similar features as described above with reference to the discussion of Claims 1 and 49, respectively. Therefore, Applicants submit that independent Claims 66 and 71 are likewise patentable over the combination of *Hill* and *Harrow*, and respectfully request the Examiner withdraw this rejection to Claims 66 and 71.

## D. <u>Dependent Claims</u>

Each of Claims 4, 6, 60-65, 67-70, and 72-80 depends directly or indirectly from one of the independent claims discussed above. Accordingly, for at least the reasons discussed above with respect to the independent claims, Applicants submit that the dependent claims are likewise patentable over the documents cited by the Examiner. The dependent claims also recite additional features that further define the claimed invention over at least the documents cited by the Examiner. Applicants submit that the documents cited by the Examiner do not disclose, teach, suggest, or make obvious integrating any of those additional features into the presently claimed invention. Accordingly, Applicants request separate and individual consideration of each dependent claim.

## V. No Waiver

Applicants have not addressed each specific rejection of the independent and dependent claims because Applicants submit that the independent claims are allowable, as discussed above. Applicants have not acquiesced to any such claim rejections and reserve the right to address the patentability of any additional claim features in the future.

## CONCLUSION

The foregoing is submitted as a full and complete response to the Office Action mailed on May 18, 2010. Applicants submit that this application is in condition for allowance and respectfully requests such action. If any issues exist that can be resolved with an Examiner's Amendment or a telephone conference, please contact Applicants' undersigned attorney at 404.572.2888.

Respectfully submitted,
KING & SPALDING LLP
By:

/W. Scott Petty/

W. Scott Petty
Registration No. 35,645

King & Spalding LLP
1180 Peachtree Street, N.E. - 34th Floor
Atlanta, Georgia 30309
Telephone: (404) 572-4600